

REMARKS

In response to the Office Action dated November 8, 2005, Applicants respectfully request reconsideration and withdrawal of the rejections of the claims.

Claims 4-8 and 10-14 were objected to under 35 C.F.R. §1.75(c), as allegedly failing to further limit the subject matter of a previous claim. The basis for this objection is not understood. Claims 4-8 depend from independent claim 3. This independent claim recites a generic device that executes the steps recited in the claim. Claims 4-8 recite individual species of this generic device. For instance, claim 4 recites that the device is a smart card, claim 5 recites that the device is a contactless card, and so forth. Accordingly, it is respectfully submitted that each of claims 4-8 further limits the subject matter recited in claim 3. Similar considerations apply to claims 10-14, relative to independent claim 9.

The objection appears to be directed to the fact that claims 4-8 and 10-14 recite an "electronic" device. Upon review of the claims, it was noted that the word "electronic" was inadvertently omitted from claims 3 and 9 in the previous amendment. To provide consistency in terminology, claims 3 and 9 have been amended to recite that they are directed to "a handheld, wearable, or portable electronic device." Reconsideration and withdrawal of the objection to claims 4-8 and 10-14 is respectfully requested.

Claims 1-3 and 9 were rejected under the second paragraph of 35 U.S.C. § 112, for various informalities. The Examiner is thanked for his careful review of these claims. In response thereto, claims 1-3 and 9 have been amended to remove the bases for the rejection, with one exception. The rejection of claim 2 states that it recites the limitation "[r]eplace s with s". First, it is to be noted that the complete phrase in claim 2 is "Replace

s with s XOR I". Second, antecedent basis for the variable "s" can be found in the second line of claim 2, namely "a random integer s of size 64 bits".

In view of the foregoing amendments and comments, reconsideration and withdrawal of the rejection under the second paragraph of 35 U.S.C. § 112 is respectfully requested.

Claim 1 was rejected under 35 U.S.C. § 101, as being directed to non-statutory subject matter. The rejection states that the claim manipulates abstract data and outputs the manipulated abstract data, which is not tangible. In response thereto, claim 1 has been amended to explicitly recite a tangible result of the method recited in the claim, namely the use of the values in the output sequence as keys in cryptographic operations. It is respectfully submitted that claim 1 recites statutory subject matter under the requirements of 35 U.S.C. § 101.

Although claim 2 was not rejected on this basis, it has been amended in a similar manner.

Claims 1-14 were rejected under 35 U.S.C. § 102, on the grounds that they were considered to be anticipated by the Yin patent (US 6,028,939). It is respectfully submitted that the Office Action does not set forth a proper basis for this rejection.

As set forth in MPEP §2131, "to anticipate a claim, the reference must teach every element of the claim." In rejecting claims 1-3 and 9, the Office Action refers to the Yin patent at column 5, lines 12-53 and Figure 2B, and states "Yin teaches the use of the DES algorithm in generating random numbers in an iterative manner using the Boolean operator exclusive OR." It is not apparent how this characterization of the Yin patent relates to the *claimed* subject matter.

For instance, claim 1 recites a method comprising a number of steps. The first of these steps is to encrypt a value D with the DES algorithm, using a key K , to produce an integer variable I . The next set of steps comprise replacing a random integer s with the value $s \text{ XOR } I$, encrypting this new value for s with the DES algorithm, to produce an integer variable y , calculating $y \text{ XOR } s$ to produce the variable x_j , replacing s with $y \text{ XOR } I$, and encrypting the resulting value of s with the DES algorithm, to produce a new value for s . It is not apparent from the Office Action how the Yin patent is being interpreted to disclose each of these steps. Similar arguments apply with respect to claims 2, 3 and 9.

If the rejection of these claims as being anticipated by the Yin patent is not withdrawn, the Examiner is requested to identify where the Yin patent discloses values corresponding to the claimed integers s , I , and y , and where it teaches the sequence of steps discussed above. In the absence of such a showing, it is respectfully submitted that the rejection cannot be maintained, since the Office Action fails to identify where the Yin patent teaches every element recited in the rejected claims.

With respect to claims 4-8 and 10-14, the Office Action states "the modifications to the preamble stand or fall with the claims that recite the preamble." It is not apparent what is meant by this statement, nor how it supports a rejection of anticipation. As discussed previously, claims 4-8 and 10-14 recite specific implementations of the devices defined in claims 3 and 9, respectively. In the rejections of claims 4-8 and 10-14 under 35 U.S.C. § 103, the Office Action explicitly admits that the Yin patent does not disclose these implementations. As such, the Yin patent does not teach every element recited in these claims, and therefore does not provide a basis for rejecting these claims under 35 U.S.C. § 102.

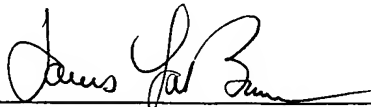
In the rejections of claims 4-8 and 10-14 under 35 U.S.C. § 103, the Office Action relies upon the Kocher et al patent (US 6,278,783) and the Farrugia published application (US 2004/0040026) as disclosing specific examples of devices in which cryptographic algorithms can be executed. However, there is no suggestion that these references disclose the elements recited in parent claims 3 and 9, from which the rejected claims depend. Since the Yin patent does not disclose this subject matter, as discussed previously, it is respectfully submitted that any combination of the Kocher and/or Farrugia references with the Yin patent does not result in the claimed subject matter.

For the foregoing reasons, it is respectfully submitted that all pending claims comply with the requirements for patentable subject matter under 35 U.S.C. §§ 101, 102, 103 and 112. Reconsideration and withdrawal of the rejections, and allowance of all claims are respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: May 5, 2006

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620